

Secure your web services

Håkan Sonesson

Senior Information Security Advisor



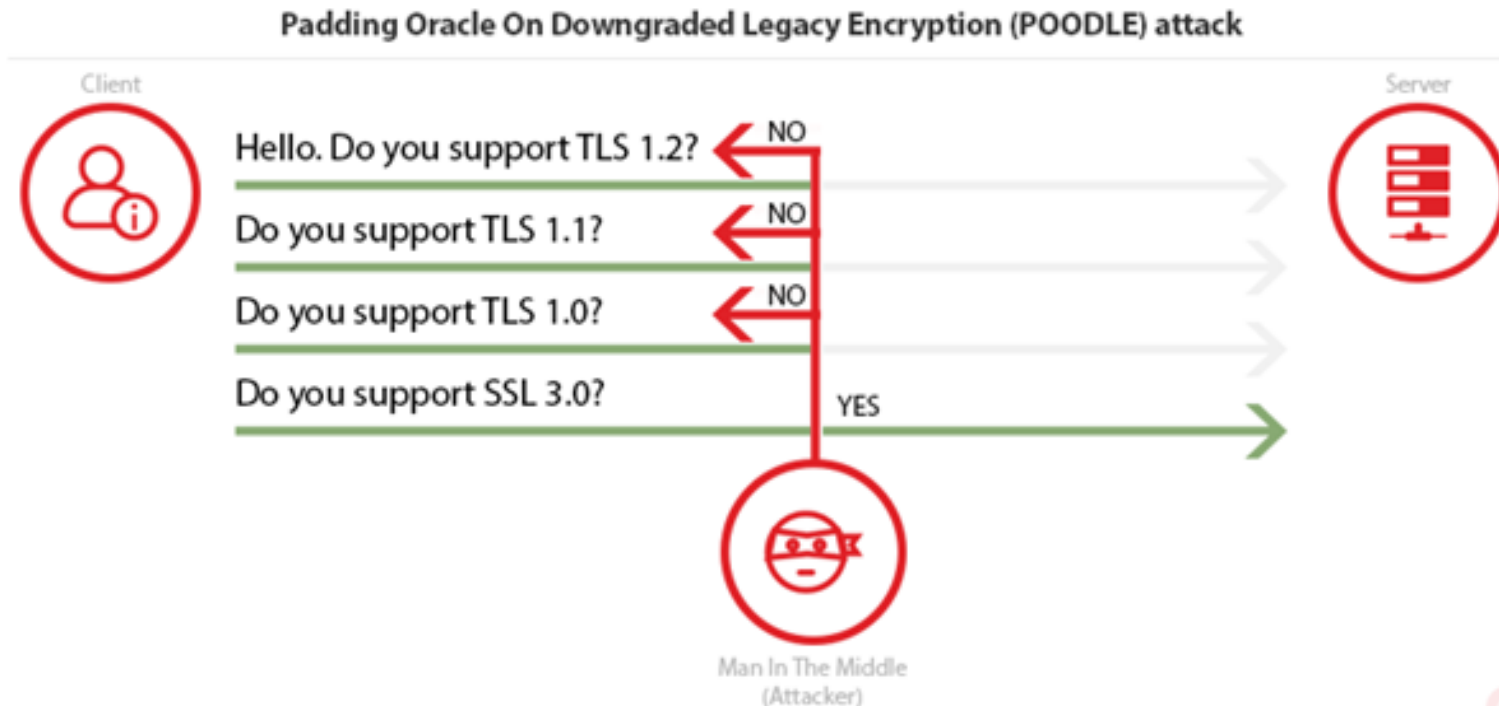
Overall perspective



Time to disable old TLS and SSL

- Time to disable **TLS 1.0**, **SSL 2.0** and **SSL 3.0**.
- Several security flaws exists:
 - **Poodle** and **DROWN**. (web traffic can be intercepted).
 - Apache: http://httpd.apache.org/docs/2.2/mod/mod_ssl.html#sslprotocol
 - Nginx: http://nginx.org/en/docs/http/nginx_http_ssl_module.html#ssl_protocols
 - IIS: <http://support2.microsoft.com/kb/187498>

Time to disable old TLS and SSL



Use the power in the configuration files

- Restrict the possibility to list content
- Protect sensitive files
 - Apache web servers use the **.htaccess** file
 - Nginx servers use **nginx.conf**
 - Microsoft IIS servers use **web.config**

Misconfigured web service



intitle:index.of site:se inurl:hidden



Index of /skspf/hidden/

Index of /skspf/hidden/. Name Last modified Size Description. up Parent Directory 17-Mar-2013 01:49 - directory docs 26-Apr-2019 20:41 - directory ...

Index of /Hidden - EWE AB

[Translate this page](#)

Index of /Hidden. Name · Last modified · Size · Description · Parent Directory, -. Ellisys/, 2016-09-13 15:51, -

Index of /Hidden/Ellisys - EWE AB

[Translate this page](#)

Name · Last modified · Size · Description · Parent Directory, -. usbex260_compliance_...> 2016-09-13 15:49, 23M. usbex260_gen_soft.zip, 2016-09-13 15:50 ...

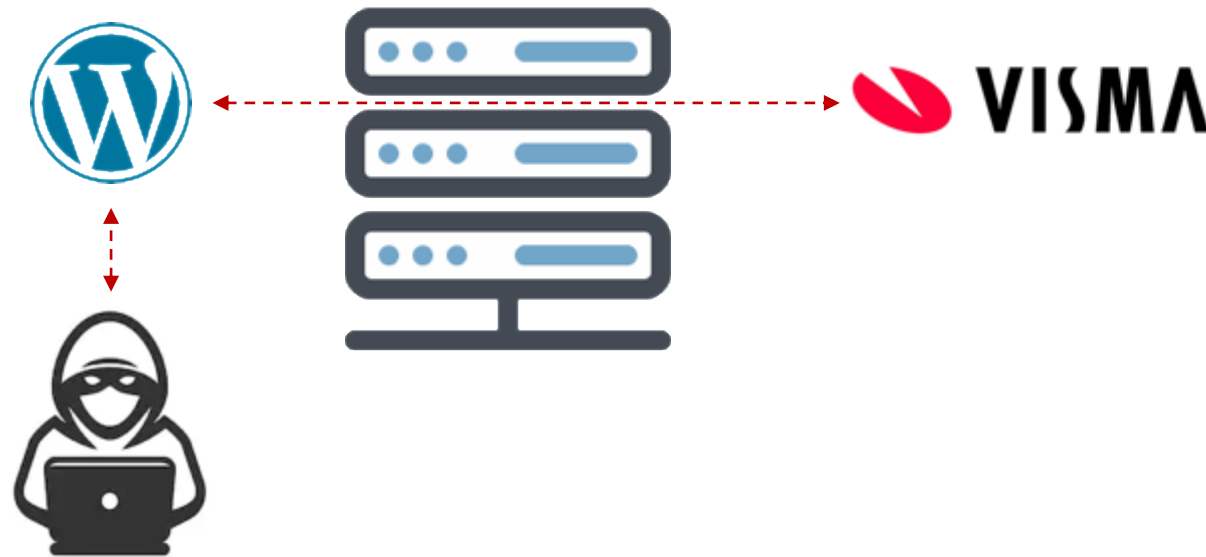
Index of /~TDDD47/include/hidden - LiU IDA

[Translate this page](#)

Name · Last modified · Size · Description. [PARENTDIR], Parent Directory, -. [TXT], defaults.sv.shtml, 2009-12-08 09:57, 552. [], menu.sv.dat, 2009-12-08 09:57 ...

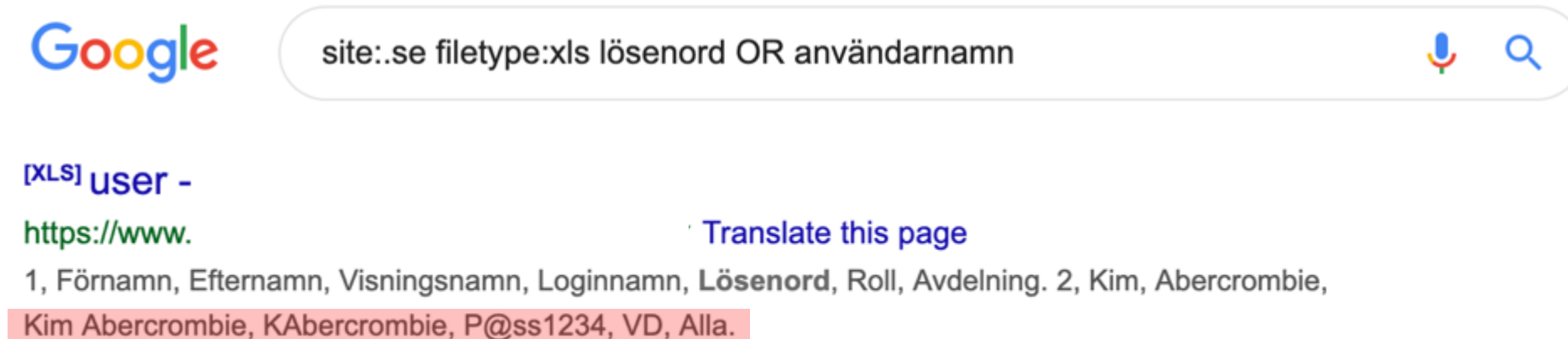
Minimize web applications

- Avoid using multiple web applications on the same web services



robots.txt and X-Robots-Tag

- Use **robots.txt** and/or **X-Robots-Tag**



```
User-agent: *  
Disallow: /ljse/  
Sitemap: http://www.lj.se/sitemap
```

robots.txt

```
Header set X-Robots-Tag "noindex, nofollow"
```

X-Robots-Tag

HTTP methods/verbs

- Disable methods/verbs, PUT and DELETE.

```
telnet 192.168.10.10 80
OPTIONS / HTTP/1.1
Host: 192.168.10.10
HTTP/1.1 200 OK
```

```
X-Powered-By: Servlet 2.4; Tomcat-5.0.28/JBoss-4.0.0 (build:
CVSTag=JBoss_4_0_0 date=200409200418)
Allow: GET, HEAD, POST, PUT, DELETE, TRACE, OPTIONS
Content-Length: 0
```


Upgrade you're web services

- Upgrade you're web services continuously

Företagshälsovården

Voice Integrate Nordic AB

Added on 2019-05-16 11:59:57 GMT

 Sweden

Technologies:



SSL Certificate

Issued By:

| - Common Name: **COMODO RSA**

Domain Validation Secure Server CA

| - Organization: **COMODO CA Limited**

Issued To:

| - Common Name: ***.medhelp.se**

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK

Cache-Control: private

Content-Length: 3583

Content-Type: text/html; charset=utf-8


















Server: Microsoft-**IIS/7.0**

X-AspNet-Version: 2.0.50727

X-Powered-By: ASP.NET

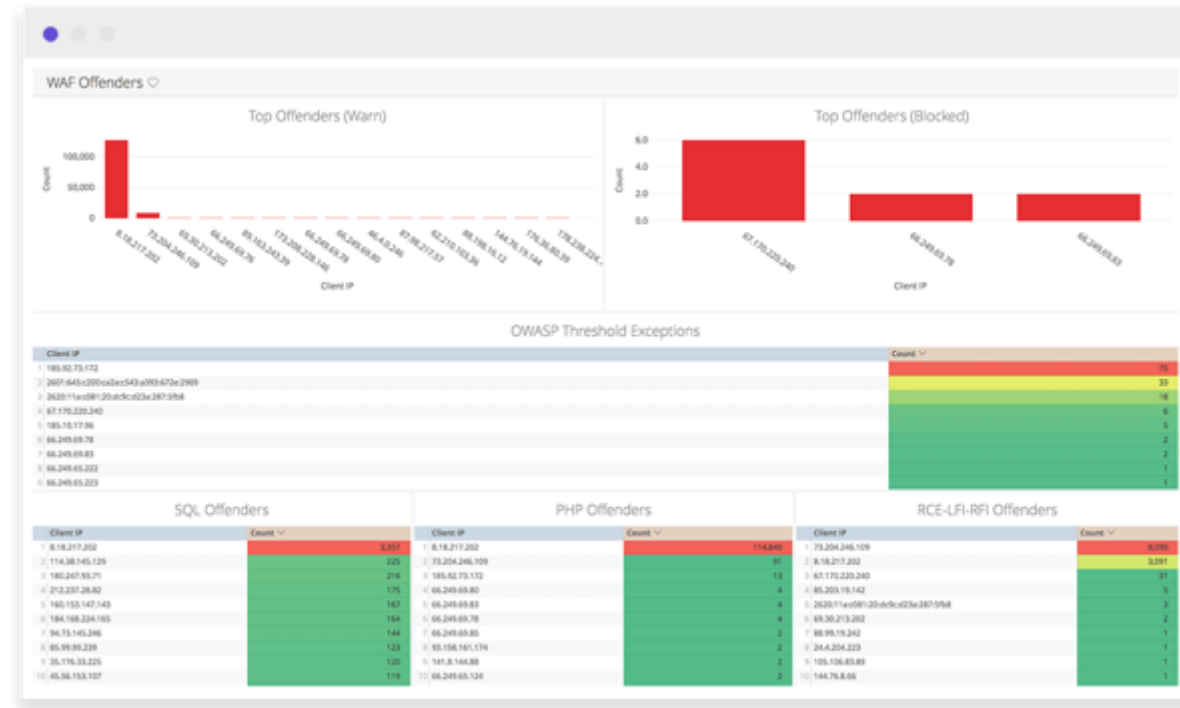
Date: Thu, 16 May 2019 11:58:23 GMT

Inspect external sources

- ▶  <https://account.psplugin.com>
- ▶  <https://app.eu.readspeaker.com>
- ▶  <https://b2b.cdon.se>
- ▶  <https://cdn-sitegainer.com>
- ▶  <https://cdn.cdon.com>
- ▶  <https://cdn.optimizely.com>
- ▶  <https://cdnjs.cloudflare.com>
- ▶  <http://cdon.dk>
- ▶  <http://cdon.fi>
- ▶  <http://cdon.no>
- ▶  <http://cdon.se>
- ▶  <https://cdon.se>
- ▶  <https://code.jquery.com>
- ▶  <http://detectportal.firefox.com>
- ▶  <https://fonts.googleapis.com>
- ▶  <https://help.cdon.com>
- ▶  <https://instagram.com>

Monitor web traffic

- Monitor web traffic. Identify abnormal behavior



Scan you're web services

